

Form PTO-1449

# INFORMATION DISCLOSURE CITATION IN AN APPLICATION

(Use several sheets if necessary)

ATTY DOCKET NO.  
2925-161PAPPLICATION  
NO  
09/127,767APPLICANT  
Sarvar PATELFILING DATE  
July 31, 1998GROUP  
2744

## U.S. PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NUMBER							DATE	NAME	CLASS	SUB CLASS	FILING DATE IF APPROPRIATE
SK	5	1	5	3	9	1	9	10/06/1992	Reeds, III et al.			

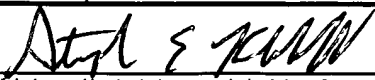
## FOREIGN PATENT DOCUMENTS

	DOCUMENT NUMBER							DATE	COUNTRY	CLASS	SUB CLASS	TRANSLATION	
												YES	NO

## OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, etc.)

SK		M. Bellare and P. Rogaway, Entity authentication and key distribution, <i>Advances in Cryptology - Crypto</i> , 1993.
		S. Bellovin and M. Merritt, Encrypted key exchange: password-based protocols secure against dictionary attacks, <i>IEEE computer society symposium on research in security and privacy</i> , 72-84 May 1992.
		R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kuttan, R. Molva, and M. Yung, Systematic design of two-party authentication protocols, <i>Advances in Cryptology - Crypto</i> , 1991.
		M. Blum and S. Micali, How to generate cryptographically strong sequences of pseudo random bits, <i>SIAM J. Computing</i> , 13 No. 4:850-864, 1984.
		R. B. Boppana and R. Hirschfeld, Pseudorandom generators and complexity classes, <i>Advances in Computing Research</i> , 5 (S. Micali, Ed.), JAI Press, CT.
		U.S. Department of Commerce/N.I.S.T., <i>Digital Signature Standard</i> , FIPS 186, May 1994.
		O. Goldreich and L. A. Levin, A hard-core predicate for all one way functions, <i>Proceedings of 21<sup>st</sup> STOC</i> , 25-32, 1989.
		S. Goldwasser and A. Micali, Probabilistic encryption, <i>Journal of Computer and Systems Science</i> , 28: 270-299, 1984.
		L. Gong, T. Lomas, R. Needham and J. Saltzer, Protecting poorly chosen secrets from guessing attacks, <i>IEEE Journal on Selected Areas in Communications</i> , 11(5): 648-656, June 1993.
		EIA/TIA, Cellular RadioTelecommunications Intersystem Operations IS-41 Rev. D, 1997.

EXAMINER



DATE CONSIDERED

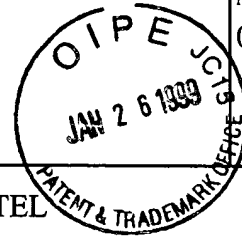
11/21/00

EXAMINER: Initial if citation considered, whether or not citation is in conformance with M.P.E.P. 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form PTO-1449

# INFORMATION DISCLOSURE CITATION IN AN APPLICATION

(Use several sheets if necessary)

ATTY DOCKET NO.  
2925-161PAPPLICATION  
NO  
09/127,767APPLICANT  
Sarvar PATELFILING DATE  
July 31, 1998GROUP  
2744

## U.S. PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB CLASS	FILING DATE IF APPROPRIATE

## FOREIGN PATENT DOCUMENTS

DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUB CLASS	TRANSLATION
					YES NO

## OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, etc.)

SK		T. Lomas, L. Gong, J. Saltzer and R. Needham, Reducing Risks from Poorly Chosen Keys, <i>Proceedings of the 12<sup>th</sup> ACM Symposium on Operating System Principles, ACM Operating Systems Review</i> , 23(5): 14-18, December 1989.
		S. Patel, Information Leakage in Encrypted Key Exchange, <i>Proceedings of DIMACS workshop on Network Threats</i> , 38: 33-40, December 1996.
		S. Patel, Number theoretic attacks on secure password schemes, <i>IEEE symposium on security and privacy</i> , 236-247, May 1997.
		S. Patel, Weaknesses of the north american wireless authentication protocol, <i>IEEE Personal Communications</i> , 40-44, June 1997.
		A. C. Yao, Theory and applications of trapdoor functions, <i>Proceedings of 23<sup>rd</sup> FOCS</i> , 80-91, 1982.
		M. Beller, L. Chang and Y. Yacobi, Privacy and authentication on a portable communication system, <i>IEEE J. Selected Areas in Communications</i> , 11(6): 821-829, 1993.
		C. Carroll, Y. Frankel and Y. Tsiounis, Efficient key distribution for slow computing devices: Achieving fast over the air activation for wireless systems, <i>IEEE symposium on security and privacy</i> , May 1998.
		TIA/EIA Interim Standard, <i>Over-the Air Service Provisioning of Mobile Stations in Spread Spectrum Systems</i> , IS-683-A, June 1998.
		E. Blossom, The VPI Protocol for Voice Privacy Devices, December 1996.
		O. Goldreich, S. Goldwasser and A. Micali, On the cryptographic applications of random functions, <i>Advances in Cryptology - Crypto</i> , 1984.
		D. Jablon, Strong Password-Only Authenticated Key Exchange, <i>ACM SIG-COMM Computer Communications Review</i> , October 1996.

EXAMINER

DATE CONSIDERED

11/21/00

EXAMINER: Initial if citation considered, whether or not citation is in conformance with M.P.E.P. 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form PTO-1449

## INFORMATION DISCLOSURE CITATION IN AN APPLICATION

(Use several sheets if necessary)

ATTY DOCKET NO.  
2925-161E

APPLICATION NO	09/127,767
-------------------	------------

APPLICANT  
**Sarvar PATEL**

FILING DATE  
July 31, 1998

GROUP	2744
-------	------

## U.S. PATENT DOCUMENTS

[illegible]

## FOREIGN PATENT DOCUMENTS

	DOCUMENT NUMBER							DATE	COUNTRY	CLASS	SUB CLASS	TRANSLATION	
												YES	NO

**OTHER DOCUMENTS** (Including Author, Title, Date, Pertinent Pages, etc.)

[illegible]

**EXAMINER**

DATE CONSIDERED

EXAMINER: Initial if citation considered, whether or not citation is in conformance with M.P.E.P. 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.